We Claim as Our Invention:

1. An electronic settlement system, comprising:

a data storage device in which value information is stored;

a client device provided with an information input and output function to the data storage device;

a store device for providing at least one of commodities and services;

a settlement management device for managing settlement between the data storage device and the store device; and

a communication system for connecting the client device, the store device, and the settlement management device so as to enable bidirectional communication;

wherein the settlement management device creates, based on settlement request information from the store device, settlement information for making settlement by the data storage device, subjects the settlement information to an encryption processing by using a common key shared by the settlement management device and the data storage device, and transmits the settlement information subjected to the encryption processing to the client device, and wherein the client device outputs the settlement information received from the settlement management device to the data storage device.

2. An electronic settlement system according to claim 1, wherein the store device creates a first signature indicating validity of the settlement request information by using a secret key of the store device, and transmits the settlement request information with the first signature to the settlement management device, and wherein the settlement management device checks validity of the first signature received from the store device by using a public key corresponding to the secret key of the store device.

3. An electronic settlement system according to claim 2, wherein the settlement request information with the first signature is transmitted to the settlement management device through the client device.

4. An electronic settlement system according to claim 2, wherein the settlement management device creates a second signature indicating validity of the settlement information with the first signature by using a secret key of the settlement management device, and transmits the settlement information given the second signature and subjected to the encryption processing to the client device, and wherein the client device checks validity of the second signature received from the settlement management device by using a public key corresponding to the secret key of the settlement management device, and then outputs the settlement information to the data storage device.

5. An electronic settlement system according to claim 1, wherein the settlement management device creates settlement completion information, creates a third signature indicating validity of the settlement completion information by using the secret key of the settlement management device, and transmits the settlement completion information including the settlement information and given the third signature to the store device, and wherein the store device checks validity of the third signature received from the settlement management device by using the public key corresponding to the secret key of the settlement management device.

6. An electronic settlement system according to claim 5, wherein the store device receives the settlement completion information with the third signature, creates settlement completion receipt information with a fourth signature by using a secret key of the store device, and transmits the settlement completion receipt information with the fourth signature to the client device, and wherein the settlement management device and the client device check validity of the fourth signature received from the store device by using a public key corresponding to the secret key of the store device.

7. An electronic settlement system according to claim 1, wherein the store device is a mall including a plurality of lower store devices.

8. A settlement management device which can update value information stored in a data storage device through a client device, comprising:

an encryption part for subjecting value update information of the data storage device to an encryption processing by using a common key shared by the settlement management device and the data storage device; and

a transmitting part for transmitting the value update information subjected to the encryption processing to the client device and, wherein the client device inputs the received value update information to the data storage device.

9. A settlement management device according to claim 8, wherein the settlement management device creates a fifth signature indicating validity of the value update information by using a secret key of the settlement management device, and transmits the value update information with the fifth signature to the client device, and wherein the client device checks validity of the fifth signature received from the settlement management device by using a public key corresponding to the secret key of the settlement management device, and then inputs the value update information to the data storage device.

10. A settlement management device for managing settlement between a data storage device which stores value information and a store device which provides at least one of commodities and services, the settlement management device comprising:

a settlement information creation part for creating, based on settlement request information from the store device, settlement information for making settlement by the data storage device;

a settlement information encryption part for subjecting the settlement information to an encryption processing by using a common key shared by the settlement management device and the data storage device; and

a settlement information output part for outputting the settlement information subjected to the encryption processing to the data storage device through a client device provided with an information input and output function to the data storage device.

11. A settlement management device according to claim 10, wherein the store device creates a first signature indicating validity of the settlement request information by using a secret key of the store device, and transmits the settlement request information with the first signature to the settlement management device, and wherein the settlement management device checks validity of the first signature received from the store device by using a public key corresponding the secret key of the store device.

12. A settlement management device according to claim 11, wherein the settlement management device creates a second signature indicating validity of the settlement information with the first signature by using a secret key of the settlement management device, and transmits the settlement information given the second signature and subjected to the encryption processing to the client device which can check validity of the second signature by using a public key corresponding to the secret key of the settlement management device and output it to the data storage device.

13. A settlement management device according to claim 10, wherein the settlement management device creates settlement completion information, creates a third signature indicating validity of the settlement completion information by using a secret key of the settlement management device, and transmits the settlement completion information including the settlement information and given the third signature to the store device which can check validity of the third signature by using a public key corresponding to the secret key of the settlement management device.

14. A settlement management device according to claim 13, wherein the store device receives the settlement completion information with the third signature, creates settlement completion receipt information with a fourth signature by using a secret key of the store device, and transmits the settlement completion receipt information with the fourth signature to the settlement management device, and wherein the settlement management device checks validity of the fourth signature

received from the store device by using a public key corresponding to the secret key of the store device.

15. A computer program for causing a computer to function as a settlement management device for updating value information stored in a data storage device through a client device, wherein the settlement management device subjects value update information of the data storage device to an encryption processing by using a common key shared by the settlement management device and the data storage device, and transmits the value update information subjected to the encryption processing to the client device, and wherein the client device inputs the received value update information to the data storage device.

16. A computer readable storage medium for storing a computer program for causing a computer to function as a settlement management device which can update value information stored in a data storage device through a client device, wherein the settlement management device subjects value update information of the data storage device to an encryption processing by using a common key shared by the settlement management device and the data storage device, and transmits the value update information subjected to the encryption processing to the client device, and wherein the client device inputs the received value update information to the data storage device.

17. A store device for providing at least one of commodities and services based on settlement made through a settlement management device between the store device and a data storage device storing value information, the store device comprising:

a settlement request information creation part for creating settlement request information;

a first signature creation part for creating a first signature indicating validity of the settlement request information by using a secret key of the store device; and

a settlement request information transmission part for transmitting the settlement request information with the first signature to the settlement management

device which can check validity of the first signature by using a public key corresponding to the secret key of the store device.

18. A store device according to claim 17, wherein the settlement management device creates, based on the settlement request information from the store device, settlement information for making settlement by the data storage device, subjects the settlement information to an encryption processing by using a common key shared by the settlement management device and the data storage device, and transmits the settlement information subjected to the encryption processing to a client device, and wherein the client device outputs the settlement information received from the settlement management device to the data storage device.

19. A store device according to claim 17, wherein the settlement request information with the first signature is transmitted from the store device to the settlement management device through a client device.

20. A store device according to claim 17, wherein the settlement management device creates settlement completion information, creates a third signature indicating validity of the settlement completion information by using a secret key of the settlement management device, and transmits the settlement completion information including the settlement information and given the third signature to the store device, and wherein the store device checks validity of the third signature received from the settlement management device by using a public key corresponding to the secret key of the settlement management device.

21. A store device according to claim 20, wherein the store device receives the settlement completion information with the third signature, creates settlement completion receipt information with a fourth signature by using the secret key of the store device, and transmits the settlement completion receipt information with the fourth signature to the settlement management device and the client device, and wherein the settlement management device and the client device check validity

of the fourth signature received from the store device by using the public key corresponding to the secret key of the store device.

22. A computer program for causing a computer to function as a store device for providing at least one of commodities and services based on settlement made through a settlement management device between the store device and a data storage device storing value information, wherein the store device includes a settlement request information creation part for creating settlement request information, a first signature creation part for creating a first signature indicating validity of the settlement request information by using a secret key of the store device, and a settlement request information transmission part for transmitting the settlement request information with the first signature to the settlement management device which can check validity of the first signature by using a public key corresponding to the secret key of the store device.

23. A computer readable storage medium for storing a computer program for causing a computer to function as a store device for providing at least one of commodities and services based on settlement made through a settlement management device between the store device and a data storage device storing value information, wherein the store device includes a settlement request information creation part for creating settlement request information, a first signature creation part for creating a first signature indicating validity of the settlement request information by using a secret key of the store device, and a settlement request information transmission part for transmitting the settlement request information with the first signature to the settlement management device which can check validity of the first signature by using a public key corresponding to the secret key of the store device.

24. A client device provided with an information input and output function to a data storage device used when settlement between a store device for providing at least one of commodities and services and the data storage device

storing value information is made through a settlement management device, the client device comprising:

a settlement information receiver part for receiving settlement information which is created by the settlement management device based on settlement request information from the store device and is subjected to an encryption processing by using a common key shared by the settlement management device and the data storage device; and

a settlement information output part for outputting the settlement information received from the settlement management device to the data storage device.

25. A data storage device storing value information used when settlement between the data storage device and a store device for providing at least one of commodities and services is made through a settlement management device, comprising a device for inputting settlement information, which is created by the settlement management device based on settlement request information from the store device and is subjected to an encryption processing by using a common key shared by the settlement management device and the data storage device, through a client device provided with an information input and output function to the data storage device.

26. A data storage device according to claim 25, wherein the data storage device is an IC card.

27. An electronic settlement method in which a client device, a store device, and a settlement management device are connected so as to enable bidirectional communication, the electronic settlement method comprising the steps of:

creating settlement information for making settlement by the data storage device storing value information, based on settlement request information from the store device;

subjecting the settlement information to an encryption processing by using a common key shared by the settlement management device and the data storage device; and

transmitting the settlement information subjected to the encryption processing to the client device.

28. An electronic settlement method according to claim 27, wherein the store device creates a first signature indicating validity of the settlement request information by using a secret key of the store device, and transmits the settlement request information with the first signature to the settlement management device, and wherein the settlement management device checks validity of the first signature received from the store device by using a public key corresponding to the secret key of the store device.